

STATE OF ALABAMA

Information Technology Standard

Standard 660-01S1: Application Security – Mobile Code

1. INTRODUCTION:

Mobile code is software obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. If used maliciously, mobile code has the potential to cause damage to information systems by introducing malware or enabling unauthorized system access.

2. OBJECTIVE:

Establish controls to prevent the development, acquisition, or introduction of unacceptable mobile code technologies onto State of Alabama information systems.

3. SCOPE:

Mobile code usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations.

4. REQUIREMENTS:

Restrictions on the implementation and use of mobile code technologies are based on the mobile code category.

4.1 CATEGORY 1 MOBILE CODE

Category 1 mobile code involves technologies having broad functionality and unmediated access to the services and resources of a computing platform. There are two subgroups of Category 1 mobile code technologies:

4.1.1 Category 1A Mobile Code

The following mobile code technologies are assigned to Category 1A:

- ActiveX controls
- Shockwave movies (including Xtras)

The use of *unsigned* Category 1A mobile code in State of Alabama information systems is prohibited.

Category 1A mobile code may only be used under the following conditions:

- The Category 1A mobile code is signed with an NSA- or NIST-approved PKI code-signing certificate
- The signed Category 1A mobile code signature is validated before executing

4.1.2 Category 1X Mobile Code

The following mobile code technologies are assigned to Category 1X:

- Mobile code scripts executing in Windows Scripting Host (WSH) (e.g., JavaScript, VBScript downloaded via URL file reference or email attachments). When JavaScript and VBScript execute within the browser, they are Category 3; however, when they execute in WSH, they are Category 1.
- HTML Applications (e.g., hta files) downloaded as mobile code
- Scrap objects (e.g., .shs and .shb files)
- Microsoft Disk Operating System (MS-DOS) batch scripts
- Unix shell scripts
- Binary executables (e.g., .exe files) downloaded as mobile code

Category 1X mobile code shall not be used in State of Alabama applications.

4.2 CATEGORY 2 MOBILE CODE

Category 2 mobile code involves technologies having full functionality, but mediated or controlled access to the services and resources of a computing platform. The following mobile code technologies are assigned to Category 2:

- Java applets and other Java mobile code
- Visual Basic for Applications (VBA) (e.g., Microsoft Office macros, also used by Corel Office)
- LotusScript (e.g., Lotus Notes scripts)
- PerfectScript (e.g., Corel Office macros)
- Postscript
- Mobile code executing in .NET Common Language Runtime

Unsigned Category 2 mobile code is required to execute in a constrained environment without access to local system and network resources (e.g., file system, Windows Registry, network connections other than to its originating server).

Unsigned Category 2 mobile code executing in a constrained execution environment without access to local system and network resources may be freely used in State of Alabama information systems.

Category 2 mobile code **not** executing in a constrained execution environment may be used only under the following conditions:

- The mobile code is obtained from an assured channel from a trusted source
- The mobile code is signed with an NSA- or NIST-approved PKI code-signing certificate
- The signed Category 2 mobile code signature is validated before executing

4.3 CATEGORY 3 MOBILE CODE

Category 3 mobile code involves technologies having limited functionality, with no capability for unmediated access to the services and resources of a computing platform.

The following mobile code technologies are assigned to Category 3:

- JavaScript, including Jscript and ECMAScript variants, when executing in the browser
- VBScript, when executing in the browser
- Portable Document Format (PDF)
- Flash animations (e.g., .swf and .spl files) executing in the Shockwave Flash Plugin

Category 3 mobile code technologies may be freely used without restrictions in State of Alabama information systems.

4.4 EMERGING MOBILE CODE

Emerging mobile code technologies refer to all mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet undergone a risk assessment and have not been assigned to one of the a risk categories above. Because of the uncertain risk, the use of emerging mobile code technologies in State of Alabama information systems is prohibited.

4.5 MOBILE CODE IN EMAIL

Mobile code can be embedded in an email body or an email attachment and downloaded as part of the actual email. Alternately, mobile code residing on a remote server can be referenced from within an email body or attachment and can be automatically downloaded and executed. Some types of mobile code execute automatically as soon as the user clicks on the message subject or previews the message; others execute when the user opens an attachment containing mobile code.

Designers shall ensure the application only embeds approved categories of mobile code in email messages.

4.6 NEW PROCUREMENT AND DEVELOPMENT EFFORTS

All new procurement and development efforts relying on mobile code technologies shall include a mobile code risk mitigation strategy detailing the measures incorporated into the system development to curtail the risk posed by its use.

4.7 EXCLUSIONS

Mobile code originating from and traveling exclusively within a single enclave boundary is exempt from these requirements.

The application need not satisfy any of the above mobile code-related requirements for the following types of mobile code:

- (1) Scripts and applets embedded in or linked to Web pages and executed in the context of the Web server (e.g., Java servlets, Java Server Pages, Java RMI, Java Jini, CGI, Active Server Pages, Cold Fusion Markup Language (CFML), PHP Hypertext Processor (PHP), Server Side Include (SSI), server-side JavaScript, and server-side LotusScript).
- (2) Local programs and command scripts (e.g., binary executables, shell scripts, batch scripts, Windows Scripting Host [WSH], Perl scripts).
- (3) Distributed object-oriented programming systems (e.g., Common Objective Request Broker Architecture [CORBA], Distributed Component Object Model [DCOM]).
- (4) Software patches, updates, including self-extracting updates and software updates that must be invoked explicitly by the user (e.g., Microsoft Windows Update).

5. ADDITIONAL INFORMATION:

5.1 POLICY

Information Technology Policy 660-01: Application Security

http://isd.alabama.gov/policy/Policy_660-01_Application_Security.pdf

5.2 RELATED DOCUMENTS

Information Technology Dictionary

http://isd.alabama.gov/policy/IT_Dictionary.pdf

Signed by Art Bess, Assistant Director

6. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	6/12/2008	